PATENT
Attorney Docket No. JP920020102US1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Masayuki NUMAO et al.	Examiner: MORSE, Gregory A.
Serial No: 10/600,547	Art Unit: 2134
Filed: June 20, 2003	
For: INFORMATION DISTRIBUTION AND PROCESSING	

APPEAL BRIEF

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The applicant submits this brief pursuant to 37 C.F.R. §41.37(a)(1) in furtherance of the Notice of Appeal filed October 9, 2007 and a Notice of Panel Decision from Pre-Appeal Brief Review dated December 14, 2007.

Please charge Deposit Account 50-0510 the $510 fee for filing this Appeal Brief. No other fee is believed due with this Appeal Brief, however, should another fee be required please charge Deposit Account 50-0510.

Real Party in Interest

The real party in interest is International Business Machines Corporation.

Related Appeals and Interferences

The Appellants' legal representative does not know of any other appeal, interference or judicial proceeding which will affect or be

directly affected by or have bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-10, 20 and 21 are pending in the present application, with claims 1, 4, 6, 9, 20 and 21 being independent claims. Claims 11-19 and 22-25 are cancelled. The rejection of claims 1-10, 20 and 21 is appealed.

Status of Amendments

No amendments to the claims were made after the Final Office Action dated July 6, 2007 ("FOA").

Summary of the Claimed Subject Matter

Independent claim 1 recites an information distribution system. App., [0032], Fig. 1. The information distribution system includes a key management server for managing secret keys and public keys corresponding to given attribute values. App., [0061], Fig. 1, item 10. A user terminal accesses the key management server to obtain attribute secret keys generated based on the secret keys. App., [0062], Fig. 1, item 30. Furthermore, the attribute secret keys correspond to attributes identifying the user terminal. App., [0050].

Claim 2 is dependent on claim 1 and recites that the provider terminal distributes the encrypted content without specifying an address of the user terminal that is to receive the encrypted content. App., [0115].

Independent claim 4 recites a server that includes a key storage for storing secret keys and public keys corresponding to predetermined attribute values. App., [0050] and Fig. 2, item 12. The server also includes an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to the set of attribute values based on secret keys corresponding to the attribute values among the secret

keys stored in the key storage. App., [0050] and Fig. 2, item 11. A sending/receiving unit receives the set of attribute values from a given user terminal and sends the attribute secret keys generated by the attribute secret key generator to the user terminal. App., [0033]. Furthermore, the attribute values identify the user terminal. App., [0045].

Independent claim 6 recites an information processing apparatus that includes a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes identifying a recipient to which a content is to be sent and using the public keys to generate criteria keys that can be decrypted by secret keys corresponding to the public keys. App., [0034], [0087] and Fig. 2, item 22. The apparatus also includes an encrypted content generator for encrypting the content based on the criteria keys. App., [0052] and Fig. 2, item 21. Furthermore, a sending unit is used to send the encrypted content without specifying any recipient of the content via a network. App., [0034].

Independent claim 9 recites an information processing apparatus receiving a content distributed over a network. App., Fig. 1. The apparatus includes a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying the information processing apparatus. App., [0036]. The attribute secret keys are generated based on the secret keys. App., [0036]. A decryptor is used to obtain an encrypted content and decrypt the content based on the attribute secret keys. App., [0054] and Fig. 2, item 32.

Independent claim 20 recites an information distribution system including a service provider managing secret keys and public keys for given attribute values. App., [0039], Fig. 8, item 800. The system also includes a plurality of user terminals for accessing the service provider to obtain attribute secret keys corresponding to attributes identifying the user terminals. App., [0039], [0062], Fig. 1, item 30. The attribute secret keys are generated based on the secret

keys. App., [0036]. Furthermore, a given one of the user terminals generates an encrypted content and sends the encrypted content to one or more of the other user terminals. App., [0041], Fig. 8, item 810. The encrypted content is decryptable by the other user terminals having the attribute secret keys corresponding to given attributes by means of the public keys. App., [0040].

Independent claim 21 recites an information distribution system including a key management server for managing secret keys and public keys for given attribute values. App., [0061], Fig. 1, item 10. The system also includes a plurality of user terminals for accessing the key management to obtain attribute secret keys corresponding to attributes identifying the user terminals. App., [0039], [0062], Fig. 1, item 30. The attribute secret keys are generated based on the secret keys. App., [0036]. Furthermore, a given one of the user terminals generates a group key and sends the group key to one or more of the other user terminals and provides a content. App., [0040], Fig. 10, item 1010. The encrypted group key is decryptable by the other user terminals having the attribute secret keys corresponding to given attributes by means of the public keys. App., [0040].

Grounds for Rejection to be Reviewed on Appeal

I. Claims 1, 3, 4, 6-10, 20 and 21 are rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent No. 6,215,877 issued to Matsumoto ("Matsumoto") in view of U.S. Patent No. 6,169,802 issued to Lerner et al. ("Lerner").

II. Claim 2 is rejected under 35 U.S.C. § 103 as obvious over Matsumoto in view of Lerner and U.S. Patent No. 5,933,605 issued to Kawano et al. ("Kawano").

III. Claim 5 is rejected under 35 U.S.C. § 103 as obvious over Matsumoto in view of Lerner and "Applicant Admittance Prior Art".

Argument

I. CLAIMS 1, 3, 4, 6-10, 20 AND 21 ARE NOT OBVIOUS UNDER 35 U.S.C. § 103 OVER MATSUMOTO IN VIEW OF LERNER

Claim 1

Claim 1 recites, part in, "a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal."

It is well settled that "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336, quoted with approval in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007).

In rejecting claim 1, the Examiner acknowledges Matsumoto (U.S. Patent No. 6,215,877) fails to disclose this claim element, but alleges such teaching can be found in Lerner (U.S. Patent No. 6,169,802). FOA, pg. 3. Specifically, the Examiner points to column 6, lines 52-62 of Lerner. The Examiner provides no explanation or reasoning for this conclusion.

The Lerner citation states,

> Creating the key based on a combination of both message data and other unique attributes relating to the messaging device is attractive because message data can often be identical. If the message data is identical, and the key is generated solely based on the message data, then the new private key may be identical to the previous one. However, if the messaging device or paging terminal finds that the new key is identical to the old key, the messaging device or terminal can manipulate the new key in a specified manner such that a unique key is generated each and every time. Lerner, col. 6, ln. 52-62.

According to Lerner, private keys are generated dynamically, based on the contents of a previously transmitted message. Lerner, col. 6, ln. 29-35. The citation makes no mention of a user terminal for accessing a key management server to obtain attribute secret keys generated based on secret keys, with attribute secret keys

corresponding to attributes identifying said user terminal.

In rejecting claim 1, the Office Action merely cites column 6, lines 52-62 of Lerner without any reasons given. The rejection does not provide articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. Furthermore, as discussed above, the teachings of Lerner directly contradict the Examiner's conclusory allegations.

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of anticipation for claim 1. The Appellants submit that the rejection of claim 1 is in error and respectfully request that the rejection of claim 1 be reversed by the honorable Board.

Claim 3

If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Claim 3 is dependent on and further limits claim 1. Since the rejection of claim 1 is believed in error, the rejection of claim 3 is also believed in error for at least the same reasons as claim 1.

Claims 4, 6, 9, 20 and 21

Claims 4, 6, 9, 20 and 21 were rejected for similar reasoning as claim 1. Thus, claims 4, 6, 9, 20 and 21 are believed allowable for at least the same reasons as claim 1.

Claims 7 and 8

Claims 7 and 8 are dependent on and further limit claim 6. Since the rejection of claim 6 is believed in error, the rejection of claims 7 and 8 is also believed in error for at least the same reasons as claim 6.

Claim 10

Claim 10 is dependent on and further limits claim 9. Since the rejection of claim 9 is believed in error, the rejection of claim 10 is also believed in error for at least the same reasons as claim 9.

II. CLAIM 2 IS NOT OBVIOUS UNDER 35 U.S.C. § 103 OVER MATSUMOTO IN VIEW OF LERNER AND KAWANO

Claim 2 recites, "The information distribution system according to claim 1, wherein said provider terminal distributes said encrypted content without specifying an address of said user terminal that is to receive said encrypted content."

In rejecting claim 2, the Examiner acknowledges Matsumoto fails to disclose the subject matter of claim 2, but alleges such teaching can be found in Kawano (U.S. Patent No. 5,933,605). FOA, pg. 7. Specifically, the Examiner points to column 11, lines 40-57 of Lerner.

The Kawano passage cited by the Examiner states,

> In the communication system using the contents code, the transmitting computer attaches to the transmission data the contents code corresponding to the contents of transmission data and then transmits the resultant data without recognizing the address of the party. A receiving computer sets data to be received on the basis of the contents code of the transmission data. Thus, the receiving computer can execute its operation without recognizing the position of itself and number of the computers as an transmission originator of the transmission data while taking only the data contents into consideration. Since each computer receives data while not specifying the data transmission originator, it is only required to broadcast the transmission data within the system and for the receiving computer to receive the data alone attached to the coincidence contents code. As a result, the data receiving operation can be carried out independently of the expansion of the system such as addition or deletion of a transmitting computer. Kawano, col. 11, ln. 40-57.

According to Kawano, a transmitting computer attaches to the transmission data the contents code corresponding to the contents of transmission data and then transmits the resultant data without recognizing the address of the party. The citation makes no mention of a provider terminal distributing encrypted content without specifying an address of a user terminal that is to receive the encrypted content.

As mentioned above, "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be

some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." In re Kahn, 441 F.3d 977, 988, 78 USPQ2d 1329, 1336, quoted with approval in KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1741, 82 USPQ2d 1385, 1396 (2007).

The Examiner provides no explanation or reasoning for the rejection beyond merely citing column 11, lines 40-57 of Kawano why the limitations of claim 2 are disclosed in Kawano. Furthermore, as discussed above, the teachings of Lerner directly contradict the Examiner's allegations. Thus, the rejection of amounts to a conclusory statement unsupported by articulated reasoning or rational underpinning. See 37 C.F.R. 1.104(c)(2).

For at least these reasons, the Appellants respectfully assert that the Examiner has not established a *prima facie* case of anticipation for claim 2. The Appellants submit that the rejection of claim 2 is in error and respectfully request that the rejection of claim 2 be reversed by the honorable Board.

III. CLAIM 5 IS NOT OBVIOUS UNDER 35 U.S.C. § 103 MATSUMOTO IN VIEW OF "APPLICANT ADMITTANCE PRIOR ART"

Claim 5 is dependent on and further limits claim 4. Since the rejection of claim 4 is believed in error, the rejection of claim 5 is also believed in error for at least the same reasons as claim 4.

Conclusion

In view of the foregoing, Appellant submits that the rejections of Claims 1-9 and 14-21 are improper and respectfully requests that the rejections of Claims 1-9 and 14-21 be reversed by the Board.

Respectfully submitted,

Dated: January 4, 2008

/ido tuchman/

Ido Tuchman, Reg. No. 45,924
Law Office of Ido Tuchman
82-70 Beverly Road
Kew Gardens, NY 11415
Telephone (718) 544-1110
Facsimile (866) 607-8538

Claims Appendix

Claim 1. (previously presented) An information distribution system comprising:

a key management server for managing secret keys and public keys corresponding to given attribute values;

a user terminal for accessing said key management server to obtain attribute secret keys generated based on said secret keys, said attribute secret keys corresponding to attributes identifying said user terminal; and

a provider terminal for generating an encrypted content that can be decrypted by said user terminal having said attribute secret keys corresponding to given attributes by means of said public keys;

wherein said provider terminal distributes said encrypted content and said user terminal decrypts said encrypted content decryptable by means of said attribute secret keys of its own.

Claim 2. (previously presented) The information distribution system according to claim 1, wherein said provider terminal distributes said encrypted content without specifying an address of said user terminal that is to receive said encrypted content.

Claim 3. (original) The information distribution system according to claim 1, wherein said user terminal sends a set of attribute values indicating attributes of its own to said key management server; and

said key management server generates said attribute secret keys unique to said user terminal based on, among said secret keys managed by said key management server, secret keys corresponding to the attribute values sent from said user terminal and sends said attribute secret keys to said user terminal.

Claim 4. (previously presented) A server comprising:

a key storage for storing secret keys and public keys

corresponding to predetermined attribute values;

an attribute secret key generator for obtaining a set of given attribute values and generating attribute secret keys corresponding to said set of attribute values based on secret keys corresponding to said attribute values among said secret keys stored in said key storage; and

a sending/receiving unit for receiving said set of attribute values from a given user terminal and sending said attribute secret keys generated by said attribute secret key generator to said user terminal; and

wherein said attribute values identifying said user terminal.

Claim 5. (previously presented) The server according to claim 4, wherein said attribute secret key generator generates said attribute secret keys by using a protocol implementing oblivious transfer protocol.

Claim 6. (previously presented) An information processing apparatus comprising:

a criteria key generator for obtaining public keys corresponding to attribute values indicating attributes identifying a recipient to which a content is to be sent and using said public keys to generate criteria keys that can be decrypted by secret keys corresponding to said public keys;

an encrypted content generator for encrypting said content based on said criteria keys; and

a sending unit for sending said encrypted content without specifying any recipient of said content via a network.

Claim 7. (original) The information processing apparatus according to claim 6, wherein said criteria key generator combines, based on predetermined rules, criteria keys corresponding to the individual attribute values encrypted by using public keys

corresponding to said individual attribute values to generate a criteria key for restricting recipients of said content.

Claim 8. (original) The information processing apparatus according to claim 6, wherein said criteria key generator generates a session key for encrypting said content and a criteria key for decrypting said session key; and

said encrypted content generator uses said session key to encrypt said content.

Claim 9. (previously presented) An information processing apparatus receiving a content distributed over a network, comprising:

a sending/receiving unit for accessing a key management server managing secret keys and public keys corresponding to given attribute values to receive attribute secret keys corresponding to attributes established for identifying said information processing apparatus, said attribute secret keys being generated based on said secret keys; and

a decryptor for obtaining an encrypted content and decrypting said content based on said attribute secret keys.

Claim 10. (currently amended) The information processing apparatus according to claim 9, wherein said sending/receiving unit sends a set of attribute values established for said information processing apparatus to said key management server and receives said attribute secret keys generated based on said set of attribute values from said key management server.

Claims 11-19 (cancelled)

Claim 20. (previously presented) An information distribution system comprising:

a service provider managing secret keys and public keys for given attribute values; and

a plurality of user terminals for accessing said service provider to obtain attribute secret keys corresponding to attributes identifying the user terminals, said attribute secret keys being generated based on said secret keys;

wherein, a given one of said user terminals generates an encrypted content and sends said encrypted content to one or more of the other user terminals, said encrypted content being decryptable by said one or more of the other user terminals having said attribute secret keys corresponding to given attributes by means of said public keys; and

said one or more of the other user terminals decrypt said encrypted content decryptable by means of said attribute secret keys of their own.

Claim 21. (previously presented) An information distribution system comprising:

a key management server for managing secret keys and public keys for given attribute values; and

a plurality of user terminals for accessing said key management server to obtain attribute secret keys corresponding to attributes identifying the user terminals, said attribute secret keys being generated based on said secret keys, wherein a given one of said user terminals generates a group key and sends said group key to ones of the other user terminals and provides a content, said encrypted group key being decryptable by said ones of the other user terminals having said attribute secret keys corresponding to given attributes by means of said public keys, said content being only accessible by using said group key.

Claims 22-25 (cancelled).

Evidence Appendix

None.

Related Proceedings Appendix

None.